

# **EXHIBIT “A”**

## **Indictment 08 Cr. 674 (SCR)**

ORIGINAL

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA :

- v. - :

RICHARD GENIN, :

Defendant. :

- - - - - x

INDICTMENT


08 Cr. 674 (SCR)

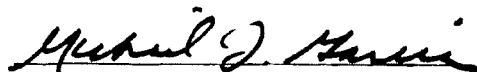
COUNT ONE

The Grand Jury charges:

1. On or about April 1, 2008, in the Southern District of New York, RICHARD GENIN, the defendant, unlawfully, willfully, and knowingly possessed a book, magazine, periodical, film, videotape, computer disk, and other material that had contained images of child pornography that had been mailed, and shipped and transported in interstate and foreign commerce by any means, including by computer, and that was produced using materials that had been mailed, and shipped and transported in interstate and foreign commerce by any means, including by computer, to wit, GENIN possessed videos containing child pornography.

(Title 18, United States Code, Sections 2252A(a)(5)(B).)

  
FOREPERSON

  
MICHAEL J. GARCIA  
United States Attorney

# **EXHIBIT “B”**

## **Complaint**

COPY

Approved: SARAH R. KRISOFF

SARAH R. KRISOFF

Assistant United States Attorney

Before: HONORABLE GEORGE A. YANTHIS  
 United States Magistrate Judge  
 Southern District of New York

-----x  
 UNITED STATES OF AMERICA

COMPLAINT

Violation of  
 18 U.S.C. § 2252A(a) (5) (B)

RICHARD GENIN,

COUNTY OF OFFENSE:  
 WESTCHESTER

Defendant.

-----x  
 SOUTHERN DISTRICT OF NEW YORK, ss.:

STEPHEN TORTORELLA, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation, and charges as follows:

COUNT ONE

On or about April 1, 2008, in the Southern District of New York, RICHARD GENIN, the defendant, unlawfully, willfully, and knowingly, did possess any book, magazine, periodical, film, videotape, computer disk, and other material that contained images of child pornography that had been mailed, shipped, and transported in interstate and foreign commerce by any means, including by computer, to wit, GENIN possessed, at least 2 dvd videos and 3 vhs tapes containing visual depictions of minors engaged in sexually explicit conduct.

(Title 18, United States Code, Section 2252A(a) (5) (B).)

The bases for my knowledge and for the foregoing charge are, in part, as follows:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and I have been involved in the investigation of the above-described offense. I am familiar with the facts and circumstances set forth below from my personal participation in the investigation, including my review of pertinent documents, and from my conversations with fellow agents.

Because this affidavit is submitted for the limited purpose of demonstrating probable cause, I have not included details of every aspect of the investigation. Where I relate statements, conversations, and actions of others, those statements, conversations, and actions are related in substance and in part, except where otherwise indicated.

#### APPLICABLE DEFINITIONS

2. The following terms have the indicated meaning in this Complaint:

a. The terms "minor," "sexually explicit conduct," "visual depiction," "child pornography," and "producing," as used herein, are defined as set forth in Title 18, United States Code, Section 2256.

#### THE INVESTIGATION

3. On or about April 1, 2008, at approximately 6:15 a.m., I, with other law enforcement officers, executed a search warrant issued by the Honorable George A. Yanthis on or about March 31, 2008, at 1 Stonelea Place, B31, New Rochelle, New York, 10801 (the "Premises"). We were seeking to find evidence of violations of Title 18, United States Code, Section 2252A(a), including but not limited to, images containing child pornography. The search warrant was based on information that, among other things, child pornography was being received at the Premises.

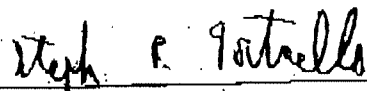
4. During the search, other law enforcement officers seized, among other things, hundreds of dvd videos and vhs tapes that appeared to contain child pornography. Law enforcement officers also seized documentation including receipts for Western Union wire transfers to a known producer of child pornography in Italy.

5. At or about the time of the search, I interviewed GENIN with two other law enforcement officers outside of the Premises. GENIN stated, in substance and in part, that he lived alone at the Premises; that he purchased child pornography from websites through a WebTV connection in the Premises; that he used numerous websites to purchase child pornography, including one website in Texas, one website in Florida, and one website in Italy; and that he used money orders and wire transfers to purchase the child pornography which were then sent to him.

5. I understand WebTV to be a service where users can access the internet through their television sets.

6. Subsequent to the search, a FBI analyst reviewed 2 dvd videos and 3 vhs tapes that were seized from the Premises and confirmed that they contain child pornography.

WHEREFORE, deponent prays that RICHARD GENIN, the defendant be imprisoned, or bailed, as the case may be.

  
STEPHEN TORTORELLA  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
\_\_\_ day of April, 2008.

UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK

# **EXHIBIT “C”**

## **Search Warrant Documents**

United States District Court		DISTRICT	
UNITED STATES OF AMERICA v. THE PREMISES KNOWN AND DESCRIBED AS 1 STONELEA PLACE, B31, NEW ROCHELLE, NY, 10801, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN		DOCKET NO.	MAGISTRATE'S CASE NO. 8 M 709
		To: Honorable George A. Yanthis United States Magistrate Judge United States Courthouse 300 Quarropas Street White Plains, New York	
The undersigned being duly sworn deposes and says: That he/she has reason to believe that			
<input type="checkbox"/> on the person of <input checked="" type="checkbox"/> on the premises		DISTRICT      SOUTHERN DISTRICT OF NEW YORK	
PREMISES KNOWN AND DESCRIBED AS  THE PREMISES KNOWN AND DESCRIBED AS 1 STONELEA PLACE, B31, NEW ROCHELLE, NY, 10801, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN			
The following property is concealed			
SEE ATTACHED AFFIDAVIT			
Affiant alleges the following grounds for search and seizure <sup>2</sup>			
SEE ATTACHED AFFIDAVIT			
<input checked="" type="checkbox"/> See attached affidavit which is incorporated as part of this affidavit for search warrant			
Affiant states the following facts establishing the foregoing grounds for issuance of a Search Warrant			
SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED AS PART OF THIS AFFIDAVIT FOR SEARCH WARRANT			
SIGNATURE OF AFFIANT		OFFICIAL TITLE, IF ANY	
		Stephen Tortorella, Federal Bureau of Investigation	
Sworn to before me, and subscribed in my presence			
DATE 3/31/09		JUDGE OR FEDERAL MAGISTRATE S/09	

<sup>1</sup> United States Judge or Judge of a State Court of Record.<sup>2</sup> If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure 41(c), show reasonable cause therefor



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----	X
	:
IN THE MATTER OF THE	:
APPLICATION OF THE UNITED	:
STATES FOR A SEARCH WARRANT	:
FOR: PREMISES KNOWN AND	:
DESCRIBED AS 1 STONELEA PLACE,	:
B31, NEW ROCHELLE, NEW YORK,	:
10801, AND CLOSED CONTAINERS	:
AND CLOSED ITEMS CONTAINED	:
THEREIN	:
	X
-----	

STATE OF NEW YORK	)
WESTCHESTER COUNTY	) ss.:
SOUTHERN DISTRICT OF NEW YORK	)

I, STEPHEN TORTORELLA, being duly sworn, depose and say:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed with the FBI since 1996. During my tenure as a Special Agent, I have conducted and participated in numerous investigations of criminal activity, including, but not limited to, criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. During the investigation of these cases, I have executed, or participated in the execution of, numerous search warrants, and seized evidence of these violations. In addition, I have received formal training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18

GENIN 000000011

U.S.C. § 2256) in all forms of media including computer media.

2. I have participated in the investigation of this matter. I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, conversations I have had with other law enforcement officers about this matter, my training and experience, and numerous discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Because this affidavit is being submitted for the limited purpose of establishing probable cause to search 1 Stonelea Place, B31, New Rochelle, New York, 10801 (henceforth the "PREMISES"), I have not included the details of every aspect of this investigation. Where actions, conversations, and statements of others are described in this affidavit, they are described in substance and in part, except where otherwise indicated.

3. I respectfully submit this affidavit in support of an application for a warrant to search the PREMISES, as described below. The instant investigation, described more fully below, has revealed that an individual, employing the email address hellmansmayo13@webtv.net, was engaged in the receipt of child pornography. Further investigation has revealed that the hellmansmayo13@webtv.net email address was registered to RICHARD GENIN ("GENIN") at the PREMISES. Based on the facts set forth in

this affidavit, there is probable cause to believe that there is presently located at the PREMISES evidence and instrumentalities of violations of federal law, including violations of 18 U.S.C. § 2252A (receiving, distributing, or promoting child pornography) and 18 U.S.C. § 2252(a)(1) (knowingly mailing or transporting child pornography). Such evidence may consist of the items set forth in Schedule A to the proposed Search Warrant. In addition, such evidence may be stored in secure locations like safety deposit boxes, safes, key-lock strong boxes, and other types of locked or closed containers in an effort to prevent the discovery or theft of said items.

#### THE PREMISES

4. I have personally observed the area near and around the PREMISES. The PREMISES are further described as follows:  
1 Stonelea Place is an apartment building complex, located on the corner of Stonelea Place and Old Boston Post Road, consisting of three separate buildings, each with a stone and brick facade. The three buildings are designated, and labeled, building "A," building "B," and building "C." Unit B31 is located on the third floor of building "B." The door of the unit is labeled "B31." The mailbox for the unit, located on the first floor of building "B," is labeled with the name RICHARD GENIN.

#### APPLICABLE DEFINITIONS

5. The following terms have the indicated meaning in

this affidavit:

a. The term "minor," "sexually explicit conduct," and "visual depiction," as used herein, are defined as set forth in 18 U.S.C. § 2256.

b. The term "child pornography," as used herein, is a visual depiction of a minor involved in sexually explicit conduct as defined in 18 U.S.C. § 2256(8)(A) and (C).

c. The term "computer," as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

d. The terms "records," "documents," and "materials" include all information recorded in any form, visual or oral, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts

from any magnetic, electrical or electronic storage device), as well as the equipment needed to record such information (including but not limited to cameras and video recording and storage devices).

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

6. I use my own computer, have personal knowledge regarding the operation of computers, and have participated in numerous investigations involving the examination of computers. I have worked extensively with computer forensic analysts. Based on this experience, and information provided to me by other law enforcement personnel involved in this investigation, I know the following:

a. The internet is a global network which allows for the sharing of data across computers attached to the network.

b. Individual users typically access the internet through a local Internet Service Provider ("ISP") (such as America Online or Verizon) using a telephone modem or other connection device, such as a cable or Digital Subscriber Line ("DSL"). When accessing the internet, the ISP will assign each user an Internet Protocol ("IP") address, a unique number used by a computer to access the internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the internet. IP addresses can also be static, whereby the user's ISP assigns the computer a unique IP address, and that

same number is used by the user every time the computer accesses the internet.

c. Communication via the internet can take place through many different media, like websites or electronic mail. Electronic mail, also known and referred to herein as "e-mail," is an electronic form of communication which can contain letter-type correspondence and graphic images. E-mail is similar to conventional paper mail in that it can be addressed from one individual to another or from one individual to many other individuals.

d. E-mail messages can contain a header that gives the screen name, the identity of the ISP, and the return address on the internet of the individual who originated the message or graphic.

e. The internet also allows individuals to trade pictures or images, often through e-mail or by downloading images from a website or another individual's computer, as described below.

(1) Photographs and other images can be stored as data on a computer. This storage can be accomplished using a "scanner," which is an optical device that can recognize images or characters on paper and, by using specialized software, convert them to digital form. This can also be accomplished by transferring photographs or files from a digital camera or

videocamera.

(2) After the photograph or other image has been scanned into the computer, the computer stores the data from the image as an individual "file." Such a file is generally known as a "GIF" (Graphic Interchange Format) or "JPEG" (for the Joint Photographic Experts Group, which wrote the standard) file, recognizable by the ".gif" or ".jpg" file extensions (hereafter referred to as an "image file").

(3) Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

(4) Using a computer connected to the internet, one can transmit and receive image files between computers located in different states or countries.

(5) An image file itself can be either a single image (one picture only, also known as a computer file), or a multiple image file (two or more pictures, usually "zipped" or compressed using a commonly available utility and recognizable by the ".zip" file extension). Multiple image files can also be placed within an executable file (recognizable by the ".exe" file extension). When a computer runs the executable file, the images can be expanded into several image files.

(6) A computer's ability to store images in digital form makes the computer an ideal repository for child

pornography. Images can be stored internally in a computer on its "hard drive," externally on "floppy" disks of several sizes and capacities, or on removable media storage devices. A single floppy disk can store dozens of images and hundreds of pages of text. The storage capacities of the electronic storage media (hard drives and floppy disks) used in home computers have grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are common. These drives can store tens of thousands of images at a very high resolution. These images can also be stored on the computers of an internet company hosting the particular website.

(7) With a modem, a computer user can transport an image file from the internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can "save" or retain the images on his computer for an indefinite time period.

(8) In addition to permanently storing the downloaded image on his computer, the user may print the image file. The finished product can be stored or distributed to other collectors. The original image that was downloaded or transported is maintained in the computer.

(9) With the modem, a computer user can also



send an image file that is retained in his computer to another individual or to areas of the internet where it can be accessed by many other computer users. This process of sending an image file is called "uploading."

(10) The process of "uploading" is similar to the "downloading" process except the user is sending the computer image file to the individual or to the internet as a whole instead of retrieving the information from another computer.

f. Another well-known component of the internet is the World Wide Web, or the "Web." The Web is a collection of websites located or stored on different computers throughout the world. Each website is identified by a unique Uniform Resource Locator ("URL"), which identifies the server on which the website information is stored. Users access websites by typing the corresponding URL into their web browser.

#### THE INVESTIGATION

##### **A. Young Video Models Websites**

7. According to a report issued by FBI, in late 2006, Italian authorities arrested an individual (henceforth, the "OPERATOR"), who operated the websites youngvideomodels.net and youngvideomodels.com (collectively, the "YVM" websites), which were used for selling and producing videos containing child pornography. After his arrest, OPERATOR provided email addresses to Italian Authorities for those individuals who purchased videos

from YVM. The Italian Authorities provided these addresses and other information about the investigation to Europol, which, in turn, provided the relevant information to law enforcement authorities in the United States. A joint investigation was commenced by the FBI, the United States Postal Inspection Service ("USPIS"), and Immigration and Customs Enforcement ("ICE") based on the information received from Europol relating to the YVM websites.

8. According to investigation reports prepared by Europol, as summarized by the FBI, visitors to youngvideomodels.net could purchase videos in two ways. If they chose to download the videos, OPERATOR would send them a web site link and password, which would be valid for a limited time; customers would use the password to access the website and download the digital video from there. Alternatively, the customer could order DVDs directly from OPERATOR which would be delivered through the mail. Customers paid for the videos by sending cash to OPERATOR, by credit card, or by paying online via electronic payment systems such as Western Union, E-Gold, or Paypal.

9. According to a dossier prepared by Europol, as summarized by the FBI, the minors in the videos that were available on youngvideomodels.net were all born in the years 1990-1998. The report indicates that in some of the videos, the

minors are depicted engaging in sexual acts, such as actual or simulated masturbation, oral sex, or simulated vaginal sex with adults or each other. It further states that in many of the videos, the minors are dressed in "string" lingerie or are completely nude, and are posed such that their genitals are the focus of the image. The videos on the web site were listed with letter and number combinations such as "D2," indicating the first initial of the victim and the number of the movie. On the web site, the lingerie worn by the girls was often auctioned to those who purchased the movies.

10. According to documents prepared by the FBI, on May 29, 2007, Europol agents provided the FBI with a hard drive containing copies of approximately 150 movies seized from OPERATOR. These movies were reviewed by an analyst from the FBI's Innocent Images Unit ("IIU"). This review concluded that all of the videos depicted females under the age of 17, some under the age of 10, a fact often demonstrated by the title screen in the videos (stating the age of the minor depicted) and by a visual review of the videos themselves. This conclusion was further verified by Europol's actual identification of these minors. At some point in the videos, nearly all of the minors appear nude or partially nude. Further, in nearly all of the videos the minors are engaged in sexual acts, or are depicted with their legs spread, or the camera lens zoomed in close on

their pubic region, thereby clearly exposing the minor's genitals.

**B. Identification of Location to be Searched**

11. According to a FBI report, in addition to providing the e-mail addresses used by individuals to communicate with OPERATOR, Europol provided the FBI with the relevant e-mail exchanges to and from OPERATOR's e-mail account. These e-mail exchanges included numerous e-mails between hellmansmayo13@webtv.net and youngvideomodels.net between August 20, 2005 and August 3, 2006.

12. According to the same FBI report, Microsoft Corporation, on behalf of WebTV Network, provided the following subscriber information regarding the e-mail address hellmansmayo13@webtv.net:

Name: Richard Genin

Address: 1 Stonelea Place 1, New Rochelle, NY

10801

Primary email address: richardgenin@webtv.net

Secondary email address: MyGenerationLP@webtv.net,  
ragingbull13@webtv.net, rickymemos@webtv.net,  
theloveyoumake@webtv.net

Telephone number: 914/636-2084

Account registered: 11/4/2000

Account Status: Active

13. According to the same FBI report, AutoTrack and Accurint searches for RICHARD GENIN ("GENIN"), provided the following information:

Name: RICHARD C. GENIN

SSAN: 096-42-4851

DOB: 05/13/1951

Address: 1 Stonelea Pl, New Rochelle, NY 10801

AutoTrack also revealed that telephone number 914-636-2084 was registered to RICHARD C. GENIN at 1 Stonelea Pl, New Rochelle, NY 10801.

14. Consolidated Edison recently confirmed that utilities have been provided to 1 Stonelea Place, #B31, since on or about June 1987, and that those utilities are registered in the name of Richard Genin, with the phone number of 914-636-2084.

**C. Hellmansmayo13@webtv.net Receives Videos From OPERATOR**

15. I have reviewed a summary, prepared by an FBI IIU analyst, of over 15 e-mails sent from hellmansmayo13@webtv.net to OPERATOR, which were found by Europol on OPERATOR's computer. Those e-mails contained, among other things, requests for certain videos, discussions about payment for videos, and commentary on the videos.

16. For example, according to the summary, the emails from hellmansmayo13@webtv.net contained the following statements:

a. In an e-mail dated 8/22/2005, the sender wrote: "Tomorrow I will go to one of the many MoneyGram locations in my city to transfer \$181.50 to you for the six videos" and "DVDs in NTSC A3, A5, AJ, N3, N6, and N16."

b. In an e-mail dated 4/8/2006, the sender wrote: "I bought 6 dvds from you last year and I'd like to buy 6 more;" "the 6 dvds in ntsc I want are. D1 Daphne 1 D2 Daphne 2 KR 1 Kristina 1 KR2 Kristina 2 LK 1 Larissa \* Kristina 1 DI1 Daphne \* Irina 1;" and "Price \$192.00."

c. In an e-mail dated 4/22/06, the sender wrote: "The two single girl videos each for Daphne and Kristina are fantastic! They are both gorgeous. I love their tiny outfits and the way they pose;" "My only minor disappointment was the two 2-girl videos. Irina blocked Daphne's body a lot, especially when applying lotion to that beautiful blonde's firm, athletic stomach. The Larisa and Kristina video had a different, 16 year old Kristina, not the 7 year old that I was expecting;" "I think Daphne and Kristina re [sic] both incredible, and Daphne is my absolute favorite. She is one of the most beautiful girls I have ever seen;" and "I would like my first custom DVD to be of Daphne."

d. In an e-mail dated 5/20/06, the sender wrote: "First, I have 18 DVDS. My favorites, in order are Daphne(2), 7 y.o. Kristina(2), Anastasya(5), Anja(1) but outfit is not skimpy

enough, Nadia(6), Daphne + Irina(1), and Larisa + 15 y.o. Kristina(1). I prefer younger girls and I like to see them move, not simply pose. My favorite DVD is Daphne #2, and 7 y.o. Kristina's videos are a very close second."

e. In an e-mail dated 5/21/06, the sender wrote:  
"Today, Sunday, May 21 at 1:10PM EDT, I sent \$206.50 to [OPERATOR] from a local Western Union office in my home city of New Rochelle" and "The Money Transfer Control Number is: 592-061-6148."

f. In an e-mail dated 8/3/2006, the sender wrote:  
"Okay, for now I will buy 7yo Kristina #4 (KR4) for \$35.50 by Western Union," and "Please keep me in mind for new videos. Remember I like younger models like 7yo Kristina, Daphne, and 9yo hidden model Angelina."

17. According to the summary, hellmansmayo13@webtv.net provided the following name and home address and phone number to youngvideomodels.net:

Richard Genin  
1 Stonelea Place, Apt. B-31  
New Rochelle, New York 10801  
Phone: (914) 636-2084

18. According to the summary, hellmansmayo13@webtv.net provided the following shipping name and address to youngvideomodels.net:

Richard Genin

Richard's Generation

2005 Palmer Avenue #131

Larchmont, New York 10538

19. According to the summary, an IIU analyst from the FBI reviewed of a number of the videos referenced in the e-mails from hellmansmayo13@webtv.net to OPERATOR. The analyst confirmed that the videos contained child pornography.

20. According to a FBI report, two undercover spam e-mail solicitations relating to child pornography were sent to hellmansmayo13@webtv.net from a USPIS Inspector. There was no response to these e-mails.

USE OF THE INTERNET, COMPUTERS, AND IMAGE AND VIDEO

RECORDING DEVICES FOR CHILD PORNOGRAPHY

21. Based on my training, experience and conversations with other law enforcement agents, I know that computers, computer technology and the internet have revolutionized the way in which child pornography is produced, distributed, utilized and collected. They have revolutionized also the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were significant



costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

22. The development of computers and the internet has added to the methods used by child pornography collectors to interact with and sexually exploit children and to produce and distribute child pornography. Computers and the internet generally serve four functions in connection with child pornography. These are: production, communication, distribution, and storage.

a. Child pornographers now can produce both still and moving images directly from a camera or a common video camera. The captured images can be edited in very similar ways to a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Further, this method of production does not leave

---

as large a trail for law enforcement to follow as have methods used in the past.

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. The development of computer technology has changed that. A modem allows any computer to connect to another computer through the use of telephone or high-speed cable lines. By connecting to a host computer, electronic contact can be made to numerous other computers around the world. Once this electronic contact is established, there are numerous outlets and ways that child pornography can be distributed over the internet.

c. Private or public internet relay chat ("IRC") channels can be and are created for the purpose of sharing child pornography. A user can log onto the IRC anonymously and "chat" and trade child pornography with other users, either on an individual or group basis. During this type of session no identifying personal information is obvious or available. The only identifiable or traceable information is the individual's IP address. IRC chatrooms are one place where pornographers meet to trade child related sexual and non-sexual stories and trade child pornography. It is also a place where children may be at risk of being "lured" to a meeting.

d. Aside from "chat rooms" that reside on many service providers' networks, ISPs often allow access to "newsgroups." Newsgroups resemble a bulletin board system where an individual can post messages along with graphic files on a public forum. Any item posted in a news group can be retrieved by any other person who has access to that particular newsgroup. One commonality between a newsgroup posting and e-mail is that they each often contain a message "header" which gives information about the account that originated a particular message or graphic files, and the return address to respond to the poster or sender.

e. Internet websites also can be used to facilitate the exchange of child pornography. A website can house child pornography directly, allowing users who access the website to view and download those images. A web site can also house an "Egroup," which is a forum by which persons with shared interests in child pornography can interact in relative privacy. Typically, most Egroups will have a moderator, and membership in the group can be open or by invitation only. Also typically, the members communicate with each other by sending an e-mail to the group, which is disseminated to all of the members. In addition, each Egroup typically has a web page that the group's members can visit to view archived postings. E-mail messages and postings

might include files that contain visual depictions and digital video clips.

f. These communication structures are ideal for the child pornography collectors. The open and anonymous communication allows the user to locate others of similar inclination and still maintain anonymity. Once contact has been established, it is possible to send text messages and graphic images to others. Moreover, the child pornography collector need not use the large service providers. Child pornography collectors can use standard internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornography collectors.

g. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred (via electronic mail, through file

transfer protocols<sup>1</sup> ("FTPs"), or via newsgroup postings) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, and easy access to the internet, the computer is a preferred method of distribution of child pornographic materials.

h. Magnetic storage located in host computers allows child pornographers to hide pornographic images from law enforcement. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image to storage on a host computer in another country. Only careful laboratory examination of electronic storage devices can recreate the evidence trail.

#### CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

23. Based on my training and experience as a Special Agent of the FBI and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the internet, with other individuals

---

<sup>1</sup> The File Transfer Protocol ("FTP") is a protocol that defines how to transfer files from one computer to another. One use, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

who have it available, or by accessing websites containing child pornography. Child pornography collectors often send and receive e-mail conversing with other collectors in order to solicit and receive child pornography.

24. I know that child pornography collectors usually maintain and possess their materials (computer and digital images, pictures, films, magazines, videotapes, correspondence, source information, etc.) in a private secure location such as their home, office, or work space, and often within a secure container. Images or videos taken off of the internet are often stored in the hard drive of the computer or on diskettes kept in private locations near the computer such as in locked desks, shelves, contiguous work space, filing cabinets or similar items and areas in office space. These images also can be printed on computer printers and maintained by child pornography collectors in paper form. Additionally, child pornography collectors often transfer those images to videotape, either by videotaping with a handheld video camera the images or videos on a computer screen, or by connecting a video cassette recorder to the computer and recording the images or videos directly.

25. Collectors of child pornography typically retain their materials and related information for many years. Most collectors of child pornography seek to increase the size of their collections in a manner similar to collectors of coins,

stamps, or rare books. Many retain these materials, including information regarding sources, for their entire adult lives. Moreover, individuals who distribute or collect child pornography generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. In addition, collectors of child pornography rarely destroy correspondence from other collectors or distributors unless their activities are uncovered by law enforcement authorities or others.

26. Based on the foregoing, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections for extended periods of time. Indeed, as noted above, based on my experience with child pornography search warrants, I know that even where information about a suspect's use of child pornography is not current, we typically find child pornography at the location of the search, assuming the suspect still resides or works there.

27. Additionally, based on my experience and training, I know that persons who collect and distribute child pornography engage in the following behavior:

a. They frequently collect sexually explicit materials in a variety of media such as photographs, magazines,

motion pictures, video tapes, books, slides and drawings or other visual media that they use for their own sexual arousal and gratification. Further, they commonly use this type of sexually explicit material to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, and to demonstrate the desired sexual acts.

b. They frequently receive sexual gratification, stimulation, and satisfaction from actual physical contact with children or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity.

c. They often correspond with or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors and collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, telephone numbers, and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

28. Based on my training and experience and my conversations with other law enforcement personnel, I have also learned that:

a. Child pornography is a permanent record of the sexual abuse of a child victim. Each time child pornography



is reproduced, downloaded, or forwarded by an internet user, the victimization of the minor appearing in the pornography is perpetuated. Such items also are important evidence and indications of an individual whose sexual objects are children, and of that individual's motive, intent, and predisposition to violate federal law related to the distribution of child pornography. Additionally, these items lead to the identification of child victims and other individuals engaging in similar conduct.

b. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify their fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities, or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-driven

behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and against self interest. The "collection" is the best indicator that law enforcement has of what the collector wants to do, not necessarily what he has done or will do. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

29. I have been informed by an Assistant U.S. Attorney that the Second Circuit has noted, "[w]hen a defendant is suspected of possessing child pornography, the staleness determination is unique because it is well known that 'images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes.'" United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (quoting United States v. Lamb, 945 F. Supp. 441, 459-60 (N.D.N.Y. 1996) (collecting cases)). In Irving, the Second Circuit upheld a search based upon information that was more than 22 months old, noting that although the affidavit disclosed that the defendant took care to destroy inappropriate photographs, "there was a fair probability that child pornography would be found. . . ." Id. Thus, under the relevant case law, information in support of probable cause in child pornography cases is often not deemed stale, even if somewhat old, because collectors and traders of

child pornography are known to store and retain their collections for extended periods of time, usually in their home and/or on their computer. See, e.g., United States v. Ricciardelli, 998 F.2d 8, 12, n. 4 (1st Cir. 1993) (stating that "history teaches that collectors [of child pornography] prefer not to dispose of their dross, typically retaining obscene materials for years"); United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000) (concluding six month old information supporting probable cause was not stale because (a) collectors of child pornography are likely to retain their sexually explicit materials; and (b) even if deleted, it is possible that the sexually explicit images could be recovered by a computer expert); United States v. Horn, 187 F.3d 781, 786-87 (8th Cir. 1999) ("lapse of time is least important when the suspected criminal activity is continuing in nature and when the property is not likely to be destroyed or dissipated" and probable cause was not stale where the defendant had demonstrated a "deep and continuing interest in his [child pornography] collection" and it was likely that he would retain child pornography for that collection).

#### REQUEST TO SEARCH THE PREMISES

30. In light of the foregoing information, and based on my experience and training, there is probable cause to believe that the PREMISES contain child pornography or other evidence concerning violations of 18 U.S.C. §§ 2252(a)(1) and 2252A,

which, among other things, make it a federal crime for any person to knowingly possess, transport or distribute child pornography, and that the fruits and instrumentalities of those violations can be found at the PREMISES. Specifically, any computers or computer equipment at the PREMISES are likely to be the primary means of accessing the internet for purposes of distributing or collecting child pornography. In addition, any cameras and videocameras may contain images and videos of child pornography. The evidence, fruits, and instrumentalities of the offenses include the items described in Schedule A to the Search Warrant.

METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS

AND COMPUTER-RELATED EQUIPMENT

31. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact discs, magnetic tapes and memory chips. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's

data in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the PREMISES. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing up to 250 gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of millions of pages of data.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file

which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentality of a crime.

32. In searching for data capable of being read, stored, or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the PREMISES, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will search and seize any computers, computer equipment and storage devices and transport these items to an appropriate law enforcement laboratory for review as to whether these items contain contraband. Because of the lengthy period of time necessary to perform a complete search of all material contained in any computers, computer equipment and storage devices, it would not be feasible to conduct this search on the PREMISES, and seizure is necessary so that the preservation of data is not jeopardized. The computers, computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

b. If, upon the search of the computers, computer equipment and storage devices it is determined that the

computer equipment and storage devices do not contain contraband, then the computer personnel will return the computer equipment and storage devices to the PREMISES.

c. The analysis of electronically-stored data may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

33. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the offense specified above.



34. In searching the data, the computer personnel may examine all of the data contained in the computers, computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the data falls within the list of items to be seized as set forth in this affidavit.

35. If the computer personnel determine that the computers, computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41, the Government will return these items, upon request.

36. In order to search for data from computers, computer equipment and storage devices, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

a. any computers, computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

b. any computers, computer equipment and storage device used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment,

modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical discs, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, cameras and videocameras;

d. any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

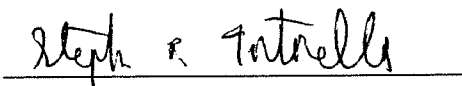
f. any physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices, or data; and

g. any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data.

37. In addition, law enforcement personnel will need to seize and search any device that can capture or store a photographic or video image.

CONCLUSION

38. Based on the foregoing, I respectfully request that the Search Warrant sought in this affidavit issue pursuant to Rule 41 of the Federal Rules of Criminal Procedure, permitting authorized agents or officers to enter the PREMISES and therein to search for and seize the items listed in Schedule A to the Search Warrant.

A handwritten signature in cursive script, reading "Steph. R. Tortorella", is written over a horizontal line.

STEPHEN TORTORELLA

Special Agent

Federal Bureau of Investigation

Sworn to before me this

th day of March, 2008

---

UNITED STATES MAGISTRATE JUDGE

SOUTHERN DISTRICT OF NEW YORK

Schedule A

1. Records, documents, and materials, including but not limited to, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, videocameras, scanners in addition to computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, RM and MPEG), and the data within the aforesaid objects relating to said materials, which may be, or are, used to: visually depict child pornography; contain information pertaining to the interest in child pornography, or sexual activity with children; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography.
2. Originals and copies of photographs, negatives, magazines, motion pictures, video tapes, books, slides, audiotapes,

handwritten notes, drawings and/or other visual media that depict what appears to be a minor engaged in sexually explicit conduct.

3. Any device that can capture or store a photographic or video image, including but not limited cameras, videocameras, and cellular telephones that are capable of capturing video images.
4. Envelopes, letters, and other correspondence, including without limitation, electronic mail, chat logs, and electronic messages, pertaining to the possession, receipt, distribution and/or reproduction of visual depictions of what appears to be a minor engaged in sexually explicit conduct, or pertaining to the luring of what appears to be a minor.
5. Envelopes, letters, and other correspondence, including without limitation electronic mail, chat logs, and electronic messages, identifying persons transmitting, through interstate commerce, including by computer and/or by United States Mail or commercial mail carriers, any visual depiction of what appears to be a minor engaged in sexually explicit conduct.

6. Books, magazines, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer or by United States Mail or commercial mail carriers, of any visual depiction of what appears to be a minor engaged in sexually explicit conduct.
7. Address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, including by computer or by United States Mail or commercial mail carriers, of any visual depiction of what appears to be a minor engaged in sexually explicit conduct.
8. Envelopes, letters, and other correspondence, including without limitation electronic mail, chat logs, and electronic messages, offering to transmit through interstate commerce, including by computer or by United States Mails or commercial mail carriers, any depictions of what appears to be a minor engaged in sexually explicit conduct.

9. Diaries, notebooks, notes and other records reflecting personal contact and other activities with what appear to be minors visually depicted while engaged in sexually explicit conduct.
10. Materials and photographs depicting sexually explicit conduct with what appear to be minors, including material that may assist in the identification and location of such minors.
11. Records evidencing ownership, tenancy, and/or occupancy of the PREMISES described above.
12. Records evidencing ownership and/or use of computer equipment found in the PREMISES described above, including without limitation, sales receipts, bills for internet access, and notes in computer manuals.
13. Records which evidence membership with any website or chat room or organizations related to child pornography, including without limitation, e-mail, correspondence and envelopes, passwords, credit card bills or receipts, and handwritten notes.

14. Any safety deposit boxes, safes, key-lock strong boxes, and other types of locked or closed containers that may contain any of the items listed in paragraphs 1-13 in this Schedule A.



Request for Sealing

Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will seriously jeopardize the progress of the investigation. Accordingly, I respectfully request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



STEVE TORTORELLA  
Special Agent  
Federal Bureau of Investigations

Sworn to before me this  
th day of March, 2008

HONORABLE GEORGE A. YANTHIS  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK

## SEARCH WARRANT ON WRITTEN AFFIDAVIT

AO

(Rev.8/97)

COPY

<b>United States District Court</b>  <b>UNITED STATES OF AMERICA</b> <b>v.</b>  <b>THE PREMISES KNOWN AND DESCRIBED</b> <b>AS 1 STONELEA PLACE, B31, NEW</b> <b>ROCHELLE, NEW YORK, 10801 AND</b> <b>CLOSED CONTAINERS AND CLOSED</b> <b>ITEMS CONTAINED THEREIN</b>	DISTRICT	
	SOUTHERN DISTRICT OF NEW YORK	
	DOCKET NO.	MAGISTRATE'S CASE NO.  8M709
	To: ANY AUTHORIZED AGENT OR LAW ENFORCEMENT PERSONNEL	
<p>Affidavit(s) having been made before me by the below-named affiant that he/she has reason to believe that on the premises known and described as THE PREMISES KNOWN AND DESCRIBED AS 1 STONELEA PLACE, B31, NEW ROCHELLE, NEW YORK, 10801, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN</p> <p style="text-align: center;">SEE SCHEDULE A</p> <p>and as I am satisfied that there is probable cause to believe that the property so described is being concealed on the <del>person or</del> premises above-described and that the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit(s),</p> <p>YOU ARE HEREBY COMMANDED to search on or before <u>4-10-08</u> (not to exceed 10 days) the <del>person or</del> place named above, and any closed or locked containers or compartments therein, for the property specified, serving this warrant and making the search at any time in the day <del>or night</del> and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to <u>any authorized judicial officer</u> as required by law.</p>		
NAME OF AFFIANT  Special Agent Stephen Tortorella Federal Bureau of Investigation	SIGNATURE OF JUDGE OR U.S. MAGISTRATE  S/way	DATE/TIME ISSUED  3/31/08 4:52pm

\* If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure Rule 41(c), show reasonable cause therefor.

GENIN 000000052

RETURN

DATE WARRANT RECEIVED

DATE AND TIME WARRANT EXECUTED

COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT  
WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

## CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the warrant

---

Subscribed, sworn to, and returned before me this date.

---

Federal Judge or U.S. Magistrate

---

Date

GENIN 000000053

Schedule A

1. Records, documents, and materials, including but not limited to, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, videocameras, scanners in addition to computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, RM and MPEG), and the data within the aforesaid objects relating to said materials, which may be, or are, used to: visually depict child pornography; contain information pertaining to the interest in child pornography, or sexual activity with children; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography.
2. Originals and copies of photographs, negatives, magazines, motion pictures, video tapes, books, slides, audiotapes,

handwritten notes, drawings and/or other visual media that depict what appears to be a minor engaged in sexually explicit conduct.

3. Any device that can capture or store a photographic or video image, including but not limited cameras, videocameras, and cellular telephones that are capable of capturing video images.
4. Envelopes, letters, and other correspondence, including without limitation, electronic mail, chat logs, and electronic messages, pertaining to the possession, receipt, distribution and/or reproduction of visual depictions of what appears to be a minor engaged in sexually explicit conduct, or pertaining to the luring of what appears to be a minor.
5. Envelopes, letters, and other correspondence, including without limitation electronic mail, chat logs, and electronic messages, identifying persons transmitting, through interstate commerce, including by computer and/or by United States Mail or commercial mail carriers, any visual depiction of what appears to be a minor engaged in sexually explicit conduct.

6. Books, magazines, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases or transactions of any kind involving the transmission through interstate commerce, including by computer or by United States Mail or commercial mail carriers, of any visual depiction of what appears to be a minor engaged in sexually explicit conduct.
7. Address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce, including by computer or by United States Mail or commercial mail carriers, of any visual depiction of what appears to be a minor engaged in sexually explicit conduct.
8. Envelopes, letters, and other correspondence, including without limitation electronic mail, chat logs, and electronic messages, offering to transmit through interstate commerce, including by computer or by United States Mails or commercial mail carriers, any depictions of what appears to be a minor engaged in sexually explicit conduct.

9. Diaries, notebooks, notes and other records reflecting personal contact and other activities with what appear to be minors visually depicted while engaged in sexually explicit conduct.
10. Materials and photographs depicting sexually explicit conduct with what appear to be minors, including material that may assist in the identification and location of such minors.
11. Records evidencing ownership, tenancy, and/or occupancy of the PREMISES described above.
12. Records evidencing ownership and/or use of computer equipment found in the PREMISES described above, including without limitation, sales receipts, bills for internet access, and notes in computer manuals.
13. Records which evidence membership with any website or chat room or organizations related to child pornography, including without limitation, e-mail, correspondence and envelopes, passwords, credit card bills or receipts, and handwritten notes.

14. Any safety deposit boxes, safes, key-lock strong boxes, and other types of locked or closed containers that may contain any of the items listed in paragraphs 1-13 in this Schedule A.



AQ

## SEARCH WARRANT ON WRITTEN AFFIDAVIT

(Rev.8/97)

<b>United States District Court</b>	DISTRICT	
	SOUTHERN DISTRICT OF NEW YORK	
<b>UNITED STATES OF AMERICA</b> <b>v.</b> <b>THE PREMISES KNOWN AND DESCRIBED</b> <b>AS 1 STONELEA PLACE, B31, NEW</b> <b>ROCHELLE, NEW YORK, 10801 AND</b> <b>CLOSED CONTAINERS AND CLOSED</b> <b>ITEMS CONTAINED THEREIN</b>	DOCKET NO.	MAGISTRATE'S CASE NO.  8470A
	To: ANY AUTHORIZED AGENT OR LAW ENFORCEMENT PERSONNEL	

Affidavit(s) having been made before me by the below-named affiant that he/she has reason to believe that on the premises known and described as THE PREMISES KNOWN AND DESCRIBED AS 1 STONELEA PLACE, B31, NEW ROCHELLE, NEW YORK, 10801, AND CLOSED CONTAINERS AND CLOSED ITEMS CONTAINED THEREIN

SEE SCHEDULE A

and as I am satisfied that there is probable cause to believe that the property so described is being concealed on the ~~person or~~ premises above-described and that the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit(s),

YOU ARE HEREBY COMMANDED to search on or before \_\_\_\_\_ (not to exceed 10 days) the ~~person or~~ place named above, and any closed or locked containers or compartments therein, for the property specified, serving this warrant and making the search at any time in the day ~~or night~~ and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to any authorized judicial officer as required by law.

NAME OF AFFIANT  Special Agent Stephen Tortorella Federal Bureau of Investigation	SIGNATURE OF JUDGE OR U.S. MAGISTRATE  S/UA	DATE/TIME ISSUED  3/31/08 4:15 PM
--	---	--

\* If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure Rule 41(c), show reasonable cause therefor.

GENIN 000000059

RETURN

DATE WARRANT RECEIVED

3/31/08

DATE AND TIME WARRANT EXECUTED

4/1/08

COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT  
WITH

Richard Genin

INVENTORY MADE IN THE PRESENCE OF

Richard Genin

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

See 3 Forms FD-597

## CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the warrant

\_\_\_\_\_  
Subscribed, sworn to, and returned before me this date.\_\_\_\_\_  
Federal Judge or U.S. Magistrate\_\_\_\_\_  
Date

GENIN 000000060

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/Seized

File # **REDACTED**

On (date) 4/1/08

item(s) listed below were:

- ☐ Received From  
☐ Returned To  
☐ Released To  
☒ Seized

(Name) Richard Genin

(Street Address) One Standa Place, B-31

(City) New Rochelle, NY

Description of Item(s): letter envelope addressed to Sara Jay

paper with "Matora Denis" + Ukraine address

paper with Western Union phone number

writing titled "Lenny Bruce and the Obscenity Law"

paper with Steve Randall address

Western Union money transfer to Sergio Marzola

paper work + photos labeled Brazil Video

Western Union money transfer to Sergio Marzola dated 5/21/06

paperwork titled DVDBadGirls

paperwork for two DVD's ordered

Express Mail address label

Express Mail address label + money order receipt for East Coast Model

misc. paperwork to order from Japan, France + Russia

Marie Marino DVD paper

misc. paperwork + handwritten pages from closet\*

Rental agreement

Received By:

Richard P. Genin

(Signature) **GENIN 000000061**

Received From:

(Signature)

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
Receipt for Property Received/Returned/Released/SeizedFile # REDACTEDOn (date) 4/11/08

item(s) listed below were:

- ☐ Received From  
☐ Returned To  
☐ Released To  
☒ Seized

(Name) Richard Genin(Street Address) One Stonelea Place, B-31(City) New Rochelle, NYDescription of Item(s): 1 bag of misc. papers from bedroom (#1)1 crate of VHS tapes (#2)1 bag of VHS tapes (#3)1 bag of DVD's (#4)1 bag with assorted paperwork (#5)1 bag of DVD's (#6)Phillips Magnavox WEB TV box, serial # 44717075 (#7)Received By: SA Stephen P. Gathrell  
(Signature) GENIN 000000062Received From: \_\_\_\_\_  
(Signature)

UNITED STATES DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION

File #

On (date) 4/1/08

item(s) listed below were:

☐ Received From

☐ Returned To

☐ Released To

☒ Seized

(Name) Richard Genin

(Street Address) One Stonelea Place, B-31

(City) New Rochelle, NY

Description of Item(s): 2 bags of VHS tapes from bedroom

Received By: [Signature] Received From: [Signature]  
(Signature) GENIN 000000062 (Signature)

GEN-IN 000000063